CLAIMS

What is claimed is:

1. A method of operating a processing system on a network, the method comprising:

encrypting an identifier of a mobile device on a wireless network; and

using the encrypted identifier to validate a request from a service initiator directed to the mobile device.

2. A method as recited in claim 1, further comprising maintaining a different cryptographic key for each of a plurality of service initiators.

3. A method as recited in claim 2, further comprising using the same cryptographic key for each service initiator in a second plurality of service initiators.

4. A method as recited in claim 2, wherein said encrypting comprises selecting and using one of the cryptographic keys to encrypt the identifier, the method further comprising including the encrypted identifier in a request to a remote processing system, based on a request from the mobile device.

5. A method as recited in claim 4, wherein said using the encrypted identifier to validate a request from a service initiator comprises selecting and using one of the cryptographic keys associated with said service initiator to validate the

request.

6. A method as recited in claim 5, wherein said method is performed by a proxy server connected to the wireless network and to a wired network including the service initiator.

7. A method as recited in claim 1, wherein said encrypting comprises:

hashing the identifier with a cryptographic key; and

including the encrypted identifier in a proxy request to a remote processing system based on an initial request received from the mobile device.

8. A method as recited in claim 7, wherein said using the encrypted identifier to validate a request from a service initiator comprises using the cryptographic key to decrypt an identifier included in the request from the service initiator; and

determining whether the identifier in the request from the service initiator corresponds to the mobile device.

9. A method of operating a processing system on a network, the method comprising:

encrypting an identifier of a mobile device on a wireless network;

including the encrypted identifier in a proxy request to a remote processing system on a network, based on a request from the mobile device; and

using the encrypted identifier to control handling of requests by a plurality of remote processing systems on the network to provide information to

the mobile device.

10. A method as recited in claim 9, further comprising maintaining a different cryptographic key for each of the plurality of remote processing systems.

11. A method as recited in claim 10, wherein said using the encrypted identifier to control handling of requests comprises, for each said request by a remote processing system, using one of the cryptographic keys corresponding to the remote processing system to validate the request.

12. A method of operating a proxy on a network, the method comprising:

storing an association of service providers and cryptographic keys;

receiving a request from a mobile device, the request directed to a remote server on the network;

using the stored association to identify a cryptographic key associated with the remote server;

using the identified cryptographic key to encode an identifier of the mobile device;

incorporating the encoded identifier into a proxy request; and

sending the proxy request to the remote server on behalf of the mobile device.

13. A method as recited in claim 12, wherein said storing an association of service providers and cryptographic keys comprises storing a unique

cryptographic key for each of a plurality of service providers.

14. A method as recited in claim 13, wherein the stored association specifies a plurality of network addresses for at least one of the plurality of service providers, and wherein said using the stored association to identify a cryptographic key comprises identifying a cryptographic key associated with a network address to which the request is directed.

15. A method as recited in claim 12, wherein said using the identified cryptographic key to encode an identifier of the mobile device comprises hashing the cryptographic key with the identifier of the mobile device.

16. A method as recited in claim 12, further comprising:

receiving a request from a service initiator on the network to push information to a mobile device;

determining whether the stored association includes a cryptographic key associated with the service initiator;

if the stored association includes a cryptographic key associated with the service initiator, using said cryptographic key to decode a device identifier in the request from the service initiator;

determining whether the decoded device identifier corresponds to the mobile device; and

allowing the request from the service initiator to be fulfilled only if the

stored association includes a cryptographic key associated with the service initiator and the decoded device identifier corresponds to the mobile device.

17. A method of operating a proxy on a network, the method comprising:

storing an association of service initiators and cryptographic keys, including a plurality of cryptographic keys and one or more network addresses associated with each of the cryptographic keys;

receiving a request from a service initiator on the network to push information to a mobile device;

determining whether the stored association includes a cryptographic key associated with the service initiator;

if the stored association includes a cryptographic key associated with the service initiator, using said cryptographic key to decode a device identifier in the request from the service initiator;

determining whether the decoded device identifier corresponds to the mobile device; and

allowing the request from the service initiator to be fulfilled only if the stored association includes a cryptographic key associated with the service initiator and the decoded device identifier corresponds to the mobile client device.

18. A method as recited in claim 17, wherein said using the identified cryptographic key to encode an identifier of the mobile device comprises hashing

the cryptographic key with the identifier of the mobile device.

19. A method as recited in claim 17, further comprising:

receiving a request from the mobile device, the request directed to a network address representing a remote server on the network;

using the stored association to identify a cryptographic key associated with the remote server;

generating a proxy request based on the request received from the mobile device, by using the identified cryptographic key associated with the remote server to encode an identifier of the mobile device and incorporating the encoded identifier into the proxy request; and

sending the proxy request to the remote server on behalf of the mobile device.

20. A method of operating a proxy on a network, the method comprising:

storing an association of service providers and cryptographic keys, including a plurality of cryptographic keys and one or more network addresses associated with each of the cryptographic keys;

receiving a request from a mobile client device, the request directed to a network address representing a remote server on the network;

using the stored association to identify a cryptographic key associated with the remote server;

generating a proxy request based on the request received from the mobile

client device, by using the identified cryptographic key to encode an identifier of the mobile client device and incorporating the encoded identifier into the proxy request; and

sending the proxy request to the remote server on behalf of the mobile client device.

21. A method as recited in claim 20, wherein said using the identified cryptographic key to encode an identifier of the mobile client device comprises hashing the cryptographic key with the identifier of the mobile client device.

22. A method as recited in claim 20, further comprising:

receiving a request from a service initiator on the network to push information to the mobile client device;

determining whether the stored association includes a cryptographic key associated with the service initiator;

if the stored association includes a cryptographic key associated with the service initiator, using said cryptographic key to decode a client identifier in the request from the service initiator;

determining whether the decoded client identifier corresponds to the mobile client device; and

allowing the request from the service initiator to be fulfilled only if the stored association includes a cryptographic key associated with the service initiator and the decoded client identifier corresponds to the mobile client device.

23. A method of operating a proxy on a network, the method comprising:

storing an association of service initiators and cryptographic keys, including a plurality of cryptographic keys and one or more network addresses associated with each of the cryptographic keys;

receiving a request from a mobile client device, the request directed to a network address representing a remote server on the network;

using the stored association to identify a cryptographic key associated with the remote server;

generating a proxy request based on the request received from the mobile client device, by using the identified cryptographic key to encode an identifier of the mobile client device and incorporating the encoded identifier into the proxy request;

sending the proxy request to the remote server on behalf of the mobile client device;

receiving a request from a service initiator on the network to push information to the mobile client device;

determining whether the stored association includes a cryptographic key associated with the service initiator;

if the stored association includes a cryptographic key associated with the service initiator, using said cryptographic key to decode a client identifier in the request from the service initiator;

determining whether the decoded client identifier corresponds to the

mobile client device; and

allowing the request from the service initiator to be fulfilled only if the stored association includes a cryptographic key associated with the service initiator and the decoded client identifier corresponds to the mobile client device.

24. A method as recited in claim 23, wherein said using the identified cryptographic key to encode an identifier of the mobile client device comprises hashing the cryptographic key with the identifier of the mobile client device.

25. A method of operating a server, the method comprising:

receiving a request to provide first information to a mobile client device on a wireless network, the request including an encrypted identifier of the mobile client device;

sending the first information in response to the request, for communication to the mobile client device; and

sending a request to push second information to the mobile client device by including the encrypted identifier in the request to push the second information to the client device, such that the encrypted identifier in the request to push the second information is used to validate the request to push the second information.

26. An apparatus comprising:

means for encrypting an identifier of a mobile device on a wireless

network; and

means for using the encrypted identifier to control action upon a request from a service initiator to provide information to the mobile device.

27. An apparatus as recited in claim 26, further comprising means for maintaining a different cryptographic key for each of a plurality of service initiators.

28. An apparatus as recited in claim 27, further comprising means for using the same cryptographic key for each service initiator of a second plurality of service initiators.

29. An apparatus as recited in claim 27, wherein said means for encrypting comprises means for selecting and using one of the cryptographic keys to encrypt the identifier, the apparatus further comprising means for including the encrypted identifier in a request to a remote processing system, based on a request from the mobile device.

30. An apparatus as recited in claim 29, wherein said means for using the encrypted identifier to control action upon a request from a service initiator comprises means for selecting and using one of the cryptographic keys associated with said service initiator to validate the request.

31. An apparatus as recited in claim 30, wherein said apparatus is a proxy server

connected to the wireless network and to a wired network including the service initiator.

32. An apparatus as recited in claim 26, wherein said means for encrypting comprises:

means for hashing the identifier with a cryptographic key; and

means for including the encrypted identifier in a request to a remote processing system based on a request received from the mobile device.

33. An apparatus as recited in claim 32, wherein said means for using the encrypted identifier to control action upon a request from a service initiator comprises means for using the cryptographic key to decrypt an identifier included in the request from the service initiator; and

means for determining whether the identifier in the request from the service initiator corresponds to the mobile device.

34. A processing system coupled to a wireless network and to a wired network, the processing system comprising:

a processor; and

a storage facility coupled to the processor and storing instructions which configure the processing system to:

encrypt an identifier of a mobile device on the wireless network;

include the encrypted identifier in a proxy request to a remote

processing system on the wired network, based on a request from the mobile device; and

use the encrypted identifier to control handling of requests by a plurality of remote processing systems on the wired network to provide information to the mobile device.

35. A processing system as recited in claim 34, wherein the processing system further stores a plurality of cryptographic keys, including a different cryptographic key for each of the plurality of remote processing systems.

36. A processing system as recited in claim 35, wherein said using the encrypted identifier to control handling of requests comprises, for each said request by a remote processing system, using one of the cryptographic keys corresponding to the remote processing system to validate the request.

37. A proxy gateway connected to a wireless network and to a wired network, the proxy gateway configured to provide a plurality of mobile devices on the wireless network with access to a plurality of processing systems on the wired network, the proxy gateway comprising:

a processor; and

a storage medium having stored therein instructions which configure the proxy gateway to perform the method comprising

storing an association of service providers and cryptographic keys;

receiving a request from a mobile device on the wireless network, the request directed to a remote server on the wired network;

using the stored association to identify a cryptographic key associated with the remote server;

using the identified cryptographic key to encode an identifier of the mobile device;

incorporating the encoded identifier into a proxy request; and

sending the proxy request to the remote server on behalf of the mobile device.

38. A proxy gateway as recited in claim 37, wherein said storing an association of service providers and cryptographic keys comprises storing a unique cryptographic key for each of a plurality of service providers.

39. A proxy gateway as recited in claim 38, wherein the stored association specifies a plurality of network addresses for at least one of the plurality of service providers, and wherein said using the stored association to identify a cryptographic key comprises identifying a cryptographic key associated with a network address to which the request is directed.

40. A proxy gateway as recited in claim 37, wherein said using the identified cryptographic key to encode an identifier of the mobile device comprises hashing the cryptographic key with the identifier of the mobile device.

41. A proxy gateway as recited in claim 37, wherein said method performed by the proxy gateway further comprises:

receiving a request from a service initiator on the wired network to push information to one of the mobile devices on the wireless network;

determining whether the stored association includes a cryptographic key associated with said service initiator;

if the stored association includes a cryptographic key associated with said service initiator, using said cryptographic key to decode a device identifier in the request from said service initiator;

determining whether the decoded device identifier corresponds to said one of the mobile devices; and

allowing the request from the service initiator to be fulfilled only if the stored association includes a cryptographic key associated with said service initiator and the decoded device identifier corresponds to said one of the mobile devices.